REMARKS

The Office Action mailed on May 13, 2005, was received and its contents carefully reviewed. In response to the Office Action, Applicant amended independent claims 1 and 15 to further recite features of the proxy encoding method and to more clearly recite the limitations of the present invention. Support for these amendments may be found throughout the Specification at least on pages 5-9. Applicant respectfully submits that no new matter was introduced by these amendments. As now recited, claims 1-15 and 18-29 are currently pending and are believed to be in condition for allowance. Applicant respectfully requests reconsideration of this application in light of the above amendments and the following remarks.

A. Previous Communication

Applicant appreciates the Examiner's consideration in conducting a personal interview with Applicant's representatives on February 17, 2005, and the opportunity afforded to explain further the concept of the invention and the amended claim language presented in the previous amendment.

B. Claim Rejections under 35 U.S.C. § 102

Claims 1, 4-7, 12-15, 19-21, and 24-29 stand rejected under 35 U.S.C. § 102(e), as being anticipated by Wright, et al. U.S. Patent No. 6,084,969 (the '969 patent) as indicated beginning on page 2 of the May 13, 2005, Office Action. In view of the amendments above and the comments below, Applicant respectfully requests reconsideration and withdrawal of this rejection.

The present application is generally directed to systems and methods for delegating decryption rights without revealing private keys or message contents. A proxy encoding scheme allows a delegate to use a transfer key to essentially authorize the re-encryption of a message for another party's use without first decrypting the original message. The other party may then use their own key to decrypt the message initially encoded for the delegate. The transfer is performed in such a way that the transfer key does not explicitly reveal the decoding keys of either the delegate or the other party, or the original message.

For example, amended independent claims 1 and 15 recite methods for encrypting an original message to be passed to a recipient by way of a grantor where the methods comprise

obtaining an encrypted message representative of the original message, the encrypted message having been encrypted with a public key corresponding to the grantor according to a public key encryption scheme; generating a public proxy key based on a private key corresponding to the recipient and on the private key corresponding to the grantor, wherein the grantor's private key and the recipient's private key are combined, and the combination of the private keys is based on the public key encryption scheme and provides that it is computationally difficult to recover the recipient's private key from the public proxy key even with the knowledge of the grantor's private key; and applying the public proxy key to transform the encrypted message into a transformed message, wherein the transformed message is decryptable by the recipient using information selected from the private key corresponding to the recipient and the available public key information, wherein no clear-text message is revealed during the transformation. Claim 15 adds additional limitations to the grantor keys.

In contrast, the '969 patent discloses a method and system that adds encryption services to an existing wireless network by providing a pager proxy arranged to receive an encrypted message from a sending pager and re-package it for re-transmission to the destination pager (see col. 4, lines 8-15). The '969 patent modifies the header of the transmission packet sent by a sending pager and/or the pager proxy (see col. 9, lines 11-14). A message is initially communicated from a sender to a proxy server, encrypted using a session key, and then communicated from the proxy server to a receiver, encrypted using a new session key (see Fig. 7 and col. 13, lines 44-65). During this process, the proxy server decrypts the encrypted message it receives using the first session key, and re-encrypts the message for the recipient using the second session key (see Fig. 8 and col. 13, line 66 to col. 14, line 5). Hence, the proxy server knows the message, which is a situation that the sender and the receiver may not want to be the case. This cited portion of the '969 patent illustrates the need for proxy encryption wherein the message is not revealed during the process of proxy transformation.

The present invention solves the problem of the proxy server knowing the message, whereby proxy encryption is utilized to ensure that no clear text message is revealed during the transfer. The method of the present invention as recited, for example, in claims 1 and 15, improves upon the decrypt-and-reencrypt method disclosed by the '969 patent.

The '969 patent fails to teach the step of generating a public proxy key with the requirement on the proxy key, and applying the proxy key step to transform the encrypted

message as recited in amended independent claims 1 and 15. Instead, the cited portion of the '969 patent discloses re-encryption of the message transmitted to the receiving pager, with the original session key encrypted by a secret key shared by the sending pager (see col. 5, lines 1-4). The '969 patent teaches away from the method recited in claims 1 and 15 of the present application by employing a decrypt-reencrypt method where the transmitted message may be revealed during the transfer.

If the method of the '969 patent is considered in the context of claims 1 and 15, with the proxy server acting as a grantor and the receiver as the recipient, the '969 patent does not disclose the generating a public proxy key step with the requirement on the proxy key, and the applying the proxy key step to transform the encrypted message. Therefore, the '969 patent fails to disclose all the recited limitations of amended independent claim 1 and amended independent claim 15 of the present invention. That is, proxy encryption as recited in amended claims 1 and 15 is not disclosed. Accordingly, Applicant respectfully requests reconsideration of claims 1 and 15 and withdrawal of the rejections under 35 U.S.C. § 102(e).

With regard to claims 4-7, 12-14, 19-21, and 24-29, Applicant respectfully traverses the rejection of claims 4-7, 12-14, 19-21, and 24-29, for similar reasons as outlined above with regard to the rejection of claims 1 and 15 under 35 U.S.C. § 102(e). Dependent claims 4-7, 12-14, 19-21, and 24-29, are dependent upon amended claim 1 and amended claim 15, respectively, and thereby include all the limitations of amended independent claim 1 and independent claim 15, respectively, while reciting additional features of the present invention.

For example, claim 4 recites that the grantor performs the receiving, generating, and applying steps of claim 1. The Examiner asserts that the '969 patent discloses the limitations of claim 4 and cites column 14, lines 17-20 of the '969 patent to support this contention. However, the cited portion of the '969 patent merely discloses, "As illustrated in FIG. 9, after authenticating the information contained in field 2, the proxy server generates a new session key (step 300), encrypts the message using the new session key (step 310), assigns the original user identification..." (see col. 14, lines 17-20). However, if the proxy server were acting as the grantor, as would have to be the case to support the Examiner's assertion, then it did not perform the generating and the applying steps recited in claim 4 of the present application. In claim 4 of the present application, the generating step is to generate a public proxy key, which is different from a session key, as the proxy key has its own requirement, and the applying step is to apply the proxy key to transform the encrypted message to an encrypted message that is decryptable by the recipient. The transformation in the present

invention is on an encrypted message, which is different from using a session key to encrypt a (clear-text) message as disclosed by the '969 patent.

Therefore, Applicant respectfully submits that the cited reference fails to disclose all the elements and limitations recited in dependent claim 4 of the present application. Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of claim 4 under 35 U.S.C. § 102(e).

Similarly, dependent claims 5-7, 12-14, 19-21, and 24-29, are dependent upon amended claim 1 and amended claim 15, respectively, and thereby include all the limitations of independent claim 1 and independent claim 15, respectively, while reciting additional features of the present invention. Applicant respectfully traverses the rejection of claims 5-7, 12-14, 19-21, and 24-29, for similar reasons as outlined above with regard to the rejection of claims 1 and 15 under 35 U.S.C. § 102(e). As discussed above, Applicant respectfully submits that the cited reference fails to disclose all the elements and limitations recited in independent claim 1 and claim 15 of the present application. Therefore, the applied reference fails to disclose all the features and limitations of claims 5-7, 12-14, 19-21, and 24-29, as well.

Accordingly, Applicant respectfully submits that claims 5-7, 12-14, 19-21, and 24-29, are allowable by virtue of their dependency upon claim 1 and claim 15, respectively, as outlined above. Applicant respectfully requests reconsideration and withdrawal of the rejection of claims 5-7, 12-14, 19-21, and 24-29, under 35 U.S.C. § 102(e).

C. Claim Rejections under 35 U.S.C. § 103

Claims 2, 3, 8-11, 18, 22, and 23 stand rejected under 35 U.S.C. § 103(a), as being unpatentable over Wright, et al. U.S. Patent No. 6,084,969 (the '969 patent) in view of Mittra U.S. Patent No. 5,748,736 (the '736 patent) as indicated beginning on page 7 of the May 13, 2005, Office Action. In view of the amendments above and the comments below, Applicant respectfully requests reconsideration and withdrawal of this rejection.

With regard to claims 2, 3, 8-11, 18, 22, and 23, Applicant respectfully traverses the rejections for similar reasons as outlined above with regard to the rejection of claims 1 and 15 under 35 U.S.C. § 102(e) as discussed above. Dependent claims 2, 3, 8-11, 18, 22, and 23, are dependent upon amended claim 1 and amended claim 15, respectively, and thereby include all the limitations of amended independent claim 1 and independent claim 15, respectively, while reciting additional features of the present invention.

For example, claims 2, 3, 22, and 23 of the present application recite additional limitations that the encrypted message has been encrypted with an ElGamal or a modified ElGamal encryption scheme. The Examiner concedes that the '969 patent fails to disclose that the encrypted message has been encrypted with an ElGamal encryption scheme and relies upon the '736 patent to cure this deficiency. However, the '736 patent discloses only the use of the ElGamal signature scheme and not an ElGamal encryption scheme. The ElGamal encryption scheme (that is, a non-deterministic encryption using a public key relying upon digital logarithm) is used for encryption purposes while the ElGamal signature scheme is for source authentication and sender non-reputation purposes. The ElGamal encryption scheme and the ElGamal signature scheme employ different algorithms and computations and are not the same. Therefore, the digital signatures of the '736 patent fail to disclose the encryption scheme as recited in claims 2, 3, 22, and 23 of the present application.

As such, Applicant respectfully submits that the cited references fail to disclose all the elements and limitations recited in dependent claims 2, 3, 22, and 23 of the present application. Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of claims 2, 3, 22, and 23 under 35 U.S.C. § 103(a).

Dependent claims 8-11, and 18 similarly add additional features to independent claims 1 and 15 respectively, and thereby include all the limitations of independent claim 1 and independent claim 15, respectively, while reciting additional features of the present invention. In each of dependent claims 8-11, and 18, the '736 fails to cure the deficiencies of the '969 patent. The resulting combination, therefore, does not teach all elements and limitations of the recited claims.

To wit, with regard to claim 8 and claim 10, the cited patents do not teach that the encrypted message has two portions, the first portion encoding a generator and a random key, and the second portion encoding the original message, the public key corresponding to the grantor, and the random key. The Examiner cites column 11, lines 47-56 of the '736 patent to remedy the deficiencies of the '969 patent, but this section merely discloses:

> "Finally, the session key (SESKey1) for this embodiment of the invention is an eight character string generated by a random or pseudorandom number generator 27, which supplies the session key to functional block 28 for use in encrypting the message (MSG), to functional block 22 for inclusion in the message authentication code, and to functional block 29 for encryption together with the header data by the private key of the sender. The output of functional block 29 is supplied to functional block 30 for encryption by the public key of the server."

As can be seen from the above citation, the cited portion of the '736 patent fails to disclose all limitations of dependent claim 8 and dependent claim 10 and to cure the deficiencies of the '969 patent.

Further, with regard to claim 9 and claim 11, the cited disclosures do not teach that the applying step operates on the second portion of the encrypted message. Note that the session key is different from the proxy key, and encryption of a message id different than the transformation of an encrypted message. The Examiner cites column 14, lines 17-20 of the '736 patent to remedy the deficiencies of the '969 patent, but this section merely discloses, "As illustrated in FIG. 9, after authenticating the information contained in field 2, the proxy server generates a new session key (step 300), encrypts the message using the new session key (step 310)...."

As can be seen from the above citation, the cited portion of the '736 patent fails to disclose all limitations of dependent claim 9 and claim 11 and to cure the deficiencies of the '969 patent.

Also, with regard to claim 18, the Examiner concedes that the '969 patent fails to include a Cramer-Shoup encryption scheme and asserts that it would be obvious to use such an encryption scheme for purposes of additional security. While the use of an encryption scheme such as the Cramer-Shoup encryption scheme may be obvious to provide additional security, working out a proxy encryption scheme based on it, especially the steps of generating a proxy key and applying the proxy key to transform the encrypted message, is not, as is evidenced by the lack of the cited disclosures teaching such a method as outlined above with regard to independent claims 1 and 15.

Applicant respectfully traverses the rejection of claims 2, 3, 8-11, 18, 22, and 23, for similar reasons as outlined above with regard to the rejection of claims 1 and 15 under 35 U.S.C. § 102(e). As discussed above, Applicant respectfully submits that the cited references fail to disclose all the elements and limitations recited in independent claim 1 and independent claim 15 of the present application as well as features and limitations of the individual dependent claims discussed above. Therefore, the applied combination of references fails to disclose all the features and limitations of claims 2, 3, 8-11, 18, 22, and 23 as well.

Accordingly, Applicant respectfully submits that claims 2, 3, 8-11, 18, 22, and 23 are allowable by virtue of their dependency upon claim 1 and claim 15, respectively, as outlined above. Applicant respectfully requests reconsideration and withdrawal of the rejection of claims 2, 3, 8-11, 18, 22, and 23 under 35 U.S.C. § 103(a).

E. Conclusion

In view of the above amendments and remarks, Applicant respectfully requests the Examiner's reconsideration of this application and the timely allowance of the pending claims.

Respectfully submitted,

NIXON PEABODY, LLP

Carlos R. Villamar
Registration No. 43,224

Date: **July 11, 2005**

Customer Number: 22204
NIXON PEABODY LLP
401 9th Street, N.W., Suite 900
Washington, DC 20004
(202) 585-8000 – Telephone
(202) 585-8080 - FAX

DRS/JAP